Specifications

Standards Supported—TCP, IP, RIP, SLIP, CSLIP, ICMP, UDP, ARP, Telnet, PPP, RFC 1331, 1332, and 1334 for PPP, backward compatible with RFC 1171 and 1172

Interface—Ethernet 10 Mbps

Connectors—(1) BNC, (3) RJ-45, (8) RJ-11

Power—100 / 250 VAC, 60 / 50 Hz, 1.5 A

Size—3.5"H x 17.5"W x 12.6"D (8.9 x 44.5 x 32 cm)

The complete package

What you get when you order the NETServer.

- NETServer
- (1) Power cord
- (1) Console cable
- (8) Phone cords
- User's Manual

Ordering Information

This information will help you place your order quickly.

PRODUCT NAME	ORDER CODE
NETServer	
8-Port	LRA108V
16-Port	LRA116V
8-Port I-modem	LRA108V-ISDN
16-Port I-modem	LRA116V-ISDN

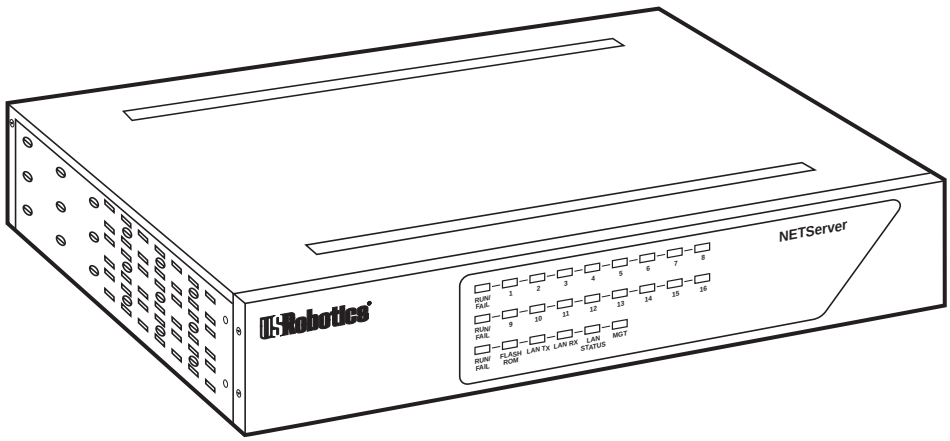
© Copyright 1996. All rights reserved
Black Box Corporation.

BLACK BOX®

The Source for Connectivity℠

NETServer

Get remote access to individual users through dialup modem connections.



The NETServer and NETServer I-modem let you gain remote access via dialup, analog, or digital lines.

Key Features

- *Access email, download files, access the internet and intranet, and interfaced with a corporate host.*
- *Software-downloadable flash ROM*
- *A solid per-user firewall guarantees security.*
- *Supports Windows 95.*
- *Share ports among users.*
- *I- models combine ISDN and modem technology in the same device.*

Overview

Now you can gain remote access to individual users through dialup lines.

The NETServer/8 and /16 let you connect to the corporate LAN to access email, download files, access Internet and Intranet web sites, and interface with the corporate host.

The NETServer/8 and 16 I-modem does everything the other NETServers do, plus it allows analog or digital calls on all ports via ISDN.

Some network devices have more than one network interface, allowing them to be attached to multiple network segments. Such devices allow data from one end of a large network to be forwarded to the other end. This process is called routing. If a packet of data must pass through more than one routing device to reach its destination, all the routing devices involved must know how to pass a packet onto the next router.

When the NETServer receives a packet that is addressed to another device, it routes that packet towards its destination. To make routing decisions, the NETServer looks up the packet's destination in its Routes Table, which contains the addresses of next routers (called "hops" or "gateways"). A gateway can be a host, a server, or any other device that performs routing functions.

Typical Applications

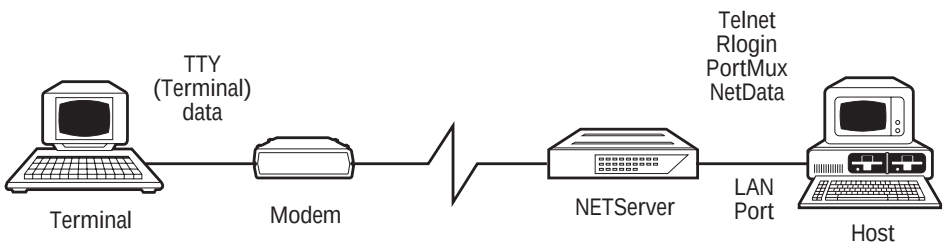
Log into an IP host via a remote terminal.

Create pools of modems that can be used by local hosts on a first-come, first-served basis.

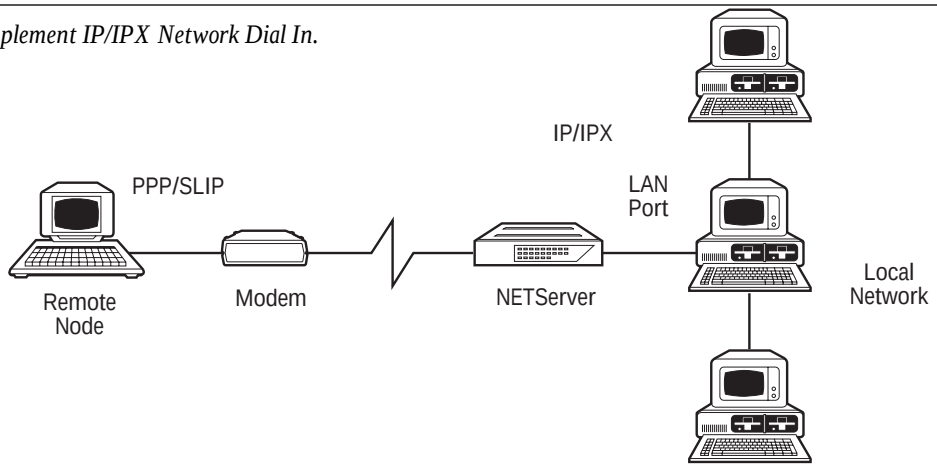
Establish dial-in or dial-up routing sessions with remote networks.

Implement four basic applications with the NETServer.

Implement IP Terminal Service.



Implement IP/IPX Network Dial In.



Technically Speaking

The NETServer allows you to implement four basic applications: IP Terminal Service, IP modem sharing, IP/IPX Network Dial In, and IP/IPX LAN-to-LAN routing. Everything else it does is based on one of these four.

IP Terminal Service

Remote terminals can log into an IP host on the NETServer's local network as if they were physically connected to it. To do this, the NETServer receives TTY terminal output (keystrokes) over a dialup line. It then forwards the terminal output to the host using a virtual terminal protocol (login service) like Telnet or Rlogin. Since the connection is bi-directional, the terminal also receives the host's responses.

IP Modem Sharing

Hosts on a local IP network can use a chassis modem to dial out. Moreover, the NETServer can create pools of modems that can be used by local hosts on a first-come, first-served basis.

To do this, the NETServer allows the host to establish a virtual terminal session with the modem. The host can then interact with the modem's command line and from there, dial out.

On a UNIX host, you can install a pseudo-TTY driver that allows the host to interact with this virtual terminal connection as if it was actually a serial port. This makes the modem appear to be directly connected to the host.

Network Dial In Access

Remote IP and IPX users can dial in and attach to the local network as if they were local nodes. IP and/or IPX packets are transmitted over a dial in connection encapsulated in a serial line networking protocol (PPP or SLIP). When received by the NETServer, the IP and IPX packets are forwarded from the remote user to the LAN and vice versa.

Dialup Routing

The same routing engine that allows network dial-in access allows the NETServer to establish dialup routing sessions with remote networks. Such connections can be maintained continuously or established on an on-demand basis and torn down when not needed.

Tech Glossary

A miniglossary for the technical terms in this brochure.

Dialup line: A temporary data connection activated by establishing a direct-dialed telephone link between two modems.

IP: Internet Protocol. The protocol used in gateways to connect networks at the OSI Network Level (Layer 3) and above.

IPX: A communication protocol in Novell NetWare that creates, maintains, and terminates connections between network devices, such as workstations and servers.

ISDN: Integrated Services Digital Network. A CCITT standard for a network that accommodates a variety of mixed digital-transmission services; the access channels are basic rate (144 Kbps) and primary rate (1.544 Mbps).

OSI: Open Systems Interconnection. An architectural model developed by the International Standards Organization (ISO) for the design of an open systems network. All communication functions are divided into seven standardized layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

Packet: A sequence of data, with associated control information, that is switched and transmitted as a whole; refers mainly to the field structure and format defined with the CCITT X.25 recommendation.

Hot Topics

How packets are routed.

When the NETServer receives a packet, it looks up the packet's destination in its routing table. If a static route is found, the packet is sent to the gateway listed. If a static route is not found, the NETServer will use a dynamic route. If the routing table contains no routes to the destination, it will send the packet to the Default Gateway. If no such gateway has been defined, the packet is discarded.

Establishing Connections to Remote Gateways

The NETServer can easily forward a packet to a gateway for which there is an established connection, such as a gateway on the same segment of the local LAN or at the other end of an active dial-up connection. All the NETServer has to do in these situations is send the packet out the right port.

However, when there is no existing connection, the NETServer has to do a bit more work. The Location table contains a list of remote gateways that the NETServer can dial into. When the NETServer does not have a connection to the packet's next hop, it looks up the address of the gateway in the Location table. The Location Table should contain a "dial script" that tells the NETServer how to contact the remote location.

Dial Scripts are most useful for on-demand routing sessions. In these situations, the NETServer connects to a remote gateway only when it has packets queued for that location.

PAP/CHAP Authentication.

The NETServer supports auto-detecting the PAP and CHAP methods of login authentication on PPP connections. If a user dials in and starts sending PPP packets, the NETServer asks that the user log in with PAP (enter a user name and password). If the user refuses PAP authentication, the NETServer demands CHAP authentication. If this is also refused, the NETServer hangs up.

PAP (Password Authentication Protocol)

PAP is simply a fancy way of saying that the dialing user or system will respond to the User Name and Password prompts given by the authenticating system. Although the NETServer will not initiate dial-out PAP authentication, you can accomplish the same effect by creating a dial script containing the expected prompts and the required responses.

However, the NETServer will respond to a dial-in PAP authentication request. All that is needed is a User Table entry for the remote device.

CHAP (Challenge Handshake Authentication Protocol)

Instead of actually sending a password over the link, CHAP relies on a "shared secret," a password that both sides of the connection know, but never send. When a remote system requests CHAP authentication, the authenticating host replies with a challenge packet. The challenge packet contains (among other things):

- A user name for the host. The challenged system needs this to look up the correct "shared secret" password.
- A "challenge value" (a randomly generated string of characters).

The challenged system then concatenates the challenge value with the shared secret and passes the new string through a hashing algorithm.

The authenticating host looks up the correct password for the user name received and then performs the same calculations the client performed, comparing the result to the response value received.